BAB III
METODE PENELITIAN

3.1 Objek Penelitian

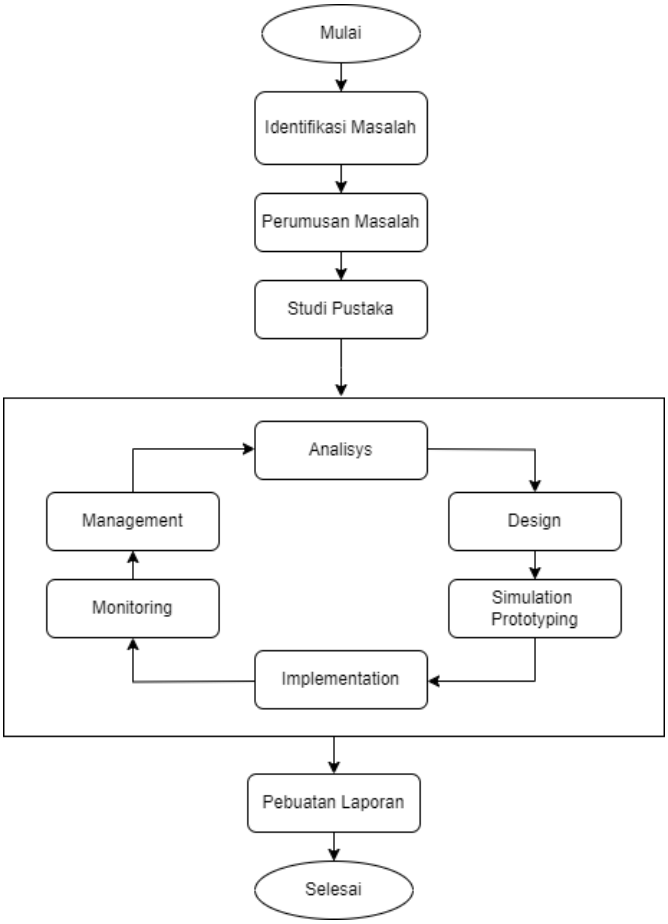
Objek penelitian dalam proses penyelesaian penelitian ini adalah untuk menyelidiki dan menganalisis implementasi IPS suricata dalam mendeteksi serta melakukan mitigasi terhadap serangan siber. Selain itu, penelitian ini bertujuan untuk mengevaluasi efektivitas penggunaan notifikasi melalui telegram dan whatsapp sebagai bagian dari sistem keamanan, dengan fokus pada kecepatan dan ketepatan respons terhadap ancaman siber yang terdeteksi. Penelitian ini juga akan memeriksa interaksi IPS suricata dengan komponen keamanan lainnya untuk menciptakan perlindungan menyeluruh. Serangan siber yang umum akan diuji untuk menguji kemampuan deteksi dan respons sistem keamanan secara keseluruhan. Kinerja keseluruhan implementasi, termasuk potensi *overhead* dan dampaknya terhadap sumber daya jaringan, juga akan menjadi fokus penelitian. Objek penelitian yang beragam ini akan memberikan gambaran menyeluruh tentang keefektifan dan keseimbangan sistem keamanan yang diusulkan dalam menghadapi ancaman siber.

3.2 Metode Penelitian

Metodologi penelitian yang digunakan dalam penelitian ini adalah *Network Development Life Cycle* (NDLC) dengan pendekatannya dalam merancang dan mengembangkan jaringan komputer secara bertahap, dengan meliputi analisis kebutuhan, perancangan, implementasi, pengujian dan pemeliharaan (Ahmad et al., 2021). Metode NDLC merupakan salah satu metode yang efektif dalam melakukan pengembangan dan analisis infrastruktur jaringan, dengan memastikan setiap langkah yang diambil memenuhi kebutuhan spesifik dan meningkatkan kinerja jaringan.

Metode NDLC melibatkan beberapa tahapan dimulai *analisys, design, simulation prototyping, implementation, monitoring, dan management* yang dapat diilustrasikan melalui suatu diagram. Diagram ini menunjukkan proses yang dilakukan selama penelitian, hanya saja dalam penelitian ini peneliti tidak

melakukan tahapan *management* karena berkaitan dengan proses pemeliharaan. Berikut merupakan metode atau alur penelitian:



Gambar 3. 1 Flowchart Metodologi Penelitian NDLC

1. Identifikasi masalah dalam penelitian ini muncul dari perlunya mengatasi ancaman serangan siber yang semakin kompleks. Peningkatan frekuensi dan kompleksitas serangan, seperti *malware*, *ransomware*, DDoS, *phishing*, dan eksploitasi identitas, menunjukkan kebutuhan mendesak untuk menerapkan solusi keamanan yang proaktif. Selain itu, rendahnya tingkat respons terhadap serangan serta dampak yang mungkin timbul memerlukan perhatian khusus dalam meningkatkan kecepatan dan efisiensi respons terhadap ancaman siber. Dengan demikian, identifikasi masalah ini menjadi dasar bagi penelitian untuk mengembangkan solusi keamanan yang lebih efektif dan responsif melalui implementasi IPS suricata dan notifikasi menggunakan telegram dan whatsapp.

2. Rumusan masalah pada penelitian ini dimulai dengan merumuskan permasalahan keamanan siber yang ingin diatasi dengan implementasi IPS suricata.
3. Studi pustaka dalam penelitian ini dimulai dengan menganalisis literatur terkait tentang implementasi IPS, deteksi serangan siber, dan notifikasi keamanan menggunakan telegram dan whatsapp. Meninjau penelitian terdahulu untuk memahami pendekatan dan solusi yang telah diusulkan.
4. Analysis dilakukan pada penelitian secara menyeluruh untuk mengidentifikasi dan memahami pola serangan siber yang mungkin terjadi. Tahap analisis melibatkan evaluasi data lalu lintas jaringan menggunakan IPS suricata, pengenalan pola perilaku yang mencurigakan, dan penilaian terhadap respons notifikasi melalui telegram dan whatsapp. Analisis tersebut memungkinkan untuk mengidentifikasi serangan, memahami cara kerja serangan tersebut, serta mengevaluasi efektivitas respons sistem. Dengan pendekatan ini, penelitian dapat menghasilkan wawasan yang mendalam tentang taktik serangan yang digunakan dan memperkuat pertahanan sistem melalui pemahaman yang lebih baik terhadap ancaman yang muncul.
5. Pada tahap ini dilakukan *design* perancangan strategi keamanan yang mencakup implementasi IPS suricata dan integrasi notifikasi melalui telegram dan whatsapp. Desain sistem mencakup topologi jaringan, penetapan kebijakan keamanan, konfigurasi IPS untuk mendeteksi dan mencegah serangan, serta pengaturan notifikasi untuk memberikan informasi real-time kepada administrator.
6. Simulation Prototyping yaitu dilakukan pembuatan model prototipe sistem keamanan dengan menggunakan IPS suricata dan notifikasi telegram dan whatsapp. Simulasi dilakukan untuk menguji desain dan fungsionalitas sistem sebelum diimplementasikan secara penuh dalam lingkungan produksi. Prototipe sistem memungkinkan untuk mensimulasikan skenario serangan siber dan mengamati responnya, serta memvalidasi efektivitas metode keamanan yang diusulkan.
7. Pada tahap *implementation* ini menerapkan solusi keamanan yang telah dirancang, yaitu IPS suricata serta notifikasi menggunakan telegram dan

whatsapp ke dalam lingkungan jaringan yang relevan. Proses implementasi mencakup instalasi dan konfigurasi perangkat lunak, penyesuaian kebijakan keamanan, serta pengaturan notifikasi. Dengan langkah ini, penelitian dapat mewujudkan solusi keamanan secara praktis dalam lingkungan nyata, sehingga sistem dapat aktif mendeteksi dan merespons serangan siber dengan menggunakan metode NDLC.

8. Monitoring dilakukan secara kontinu terhadap lalu lintas jaringan dan kejadian keamanan, memungkinkan identifikasi cepat terhadap anomali atau serangan yang terdeteksi.
9. Management yaitu proses pemeliharaan kebijakan keamanan, pembaruan perangkat lunak, serta pengelolaan notifikasi yang dihasilkan oleh IPS suricata.
10. Pembuatan laporan merupakan tahap akhir dalam metode penelitian NDLC yaitu dengan menyusun laporan penelitian yang mencakup semua langkah di atas. Laporan ini akan memuat detail implementasi, hasil pengujian, analisis, dan kesimpulan penelitian.

3.2.1 *Analysis*

3.2.1.1 Jenis dan Sumber Data

Jenis dan sumber data yang diperoleh dalam penelitian ini peneliti akan menggunakan data utama. Implementasi IPS suricata dan notifikasi telegram dan whatsapp, yaitu data utama akan diperoleh langsung dari penerapan IPS suricata serta penggunaan notifikasi telegram dan whatsapp pada sistem yang relevan. Ini mencakup hasil pengamatan, catatan, dan log yang dihasilkan selama eksperimen atau implementasi sistem keamanan. Data utama ini memberikan informasi langsung tentang respons dan kinerja sistem selama pengujian.

3.2.1.2 Teknik Pengumpulan Data

Teknik pengumpulan data pada penelitian ini melibatkan pendekatan yang komprehensif untuk mendapatkan informasi yang dibutuhkan. Berikut adalah penjelasan rinci mengenai teknik pengumpulan data yang akan digunakan:

1. Observasi yaitu dengan melibatkan pengamatan langsung terhadap implementasi IPS suricata serta notifikasi telegram dan whatsapp pada sistem

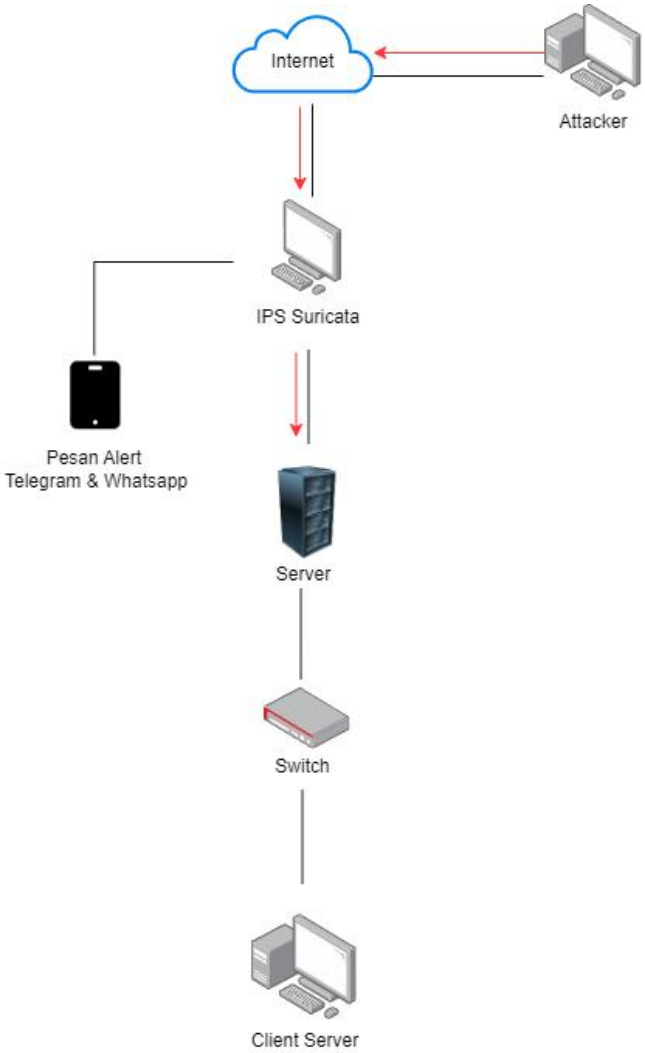
jaringan yang diuji. Observasi ini mencakup pemantauan operasional, respons terhadap serangan, dan kinerja umum sistem keamanan.

2. Analisis log yaitu dengan menganalisis log yang dihasilkan oleh IPS suricata terkait deteksi dan mitigasi serangan siber. Log ini memberikan informasi tentang jenis serangan yang terdeteksi, waktu response dan langkah-langkah yang diambil untuk mengatasi serangan.
3. Dokumentasi teknik yaitu dengan mengumpulkan informasi dari dokumentasi teknis terkait IPS suricata serta telegram dan whatsapp ini mencakup petunjuk penggunaan, catatan rilis, dan panduan konfigurasi untuk memahami implementasi dengan lebih mendalam.
4. Literatur terkait yang dengan menggunakan jurnal ilmiah, buku, dan artikel terkait implementasi IPS, deteksi serangan siber, serta notifikasi keamanan menggunakan telegram dan whatsapp untuk memberikan dasar teoritis dan kontekstual.

Penerapan berbagai teknik ini diharapkan dapat memberikan data yang kaya dan beragam, memungkinkan analisis yang mendalam terhadap efektivitas IPS suricata dalam menghadapi serangan siber dengan dukungan notifikasi melalui telegram dan whatsapp.

3.2.2 *Design*

Tahap desain peneliti melakukan perancangan topologi jaringan, di mana pada penelitian ini digunakan untuk simulasi, dengan menggunakan *Virtual Machine* (VM) yaitu *Virtual Box*. Berikut merupakan ilustrasi topologi jaringan yang akan digunakan pada penelitian ini, yang dijelaskan pada Gambar 3.2:



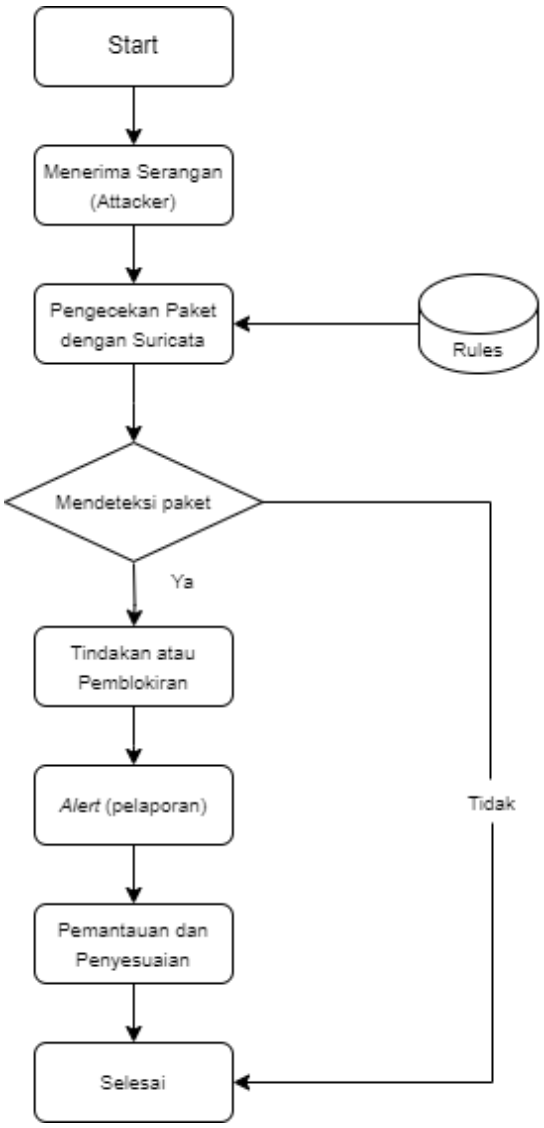
Gambar 3. 2 Topologi Jaringan

Gambar 3.2 di atas merupakan topologi jaringan yang digunakan dalam penelitian ini, di mana penyerang yang berasal dari luar jaringan akan melakukan aksi kejahatan yaitu dengan mengirimkan berbagai jenis serangan siber ke *server* atau yang akan dicoba dalam pengujian penelitian ini yaitu delapan jenis serangan dengan bantuan beberapa *tools* sesuai dengan kebutuhan masing-masing serangan. Serangan yang masuk akan dilakukan penyesuaian dengan *rule signature* yang telah dibuat pada masing-masing jenis serangan, jika sesuai maka akan terdeteksi dan dilakukan pencegahan sedini mungkin oleh IPS suricata. Kemudian, sistem akan mengirimkan notifikasi ke aplikasi telegram dan whatsapp administrator jika serangan berhasil terdeteksi dan di blokir oleh IPS suricata.

3.2.3 *Simulation*

3.2.3.1 Cara Kerja IPS Suricata

Seperti yang disebutkan sebelumnya bahwa pada penelitian ini, peneliti menggunakan IPS suricata sebagai sistem keamanan jaringan. Gambar 3.3 menjelaskan bagaimana cara kerja dari sistem IPS suricata sehingga dapat melakukan deteksi dan pencegahan pada lalu lintas jaringan yang mencurigakan.



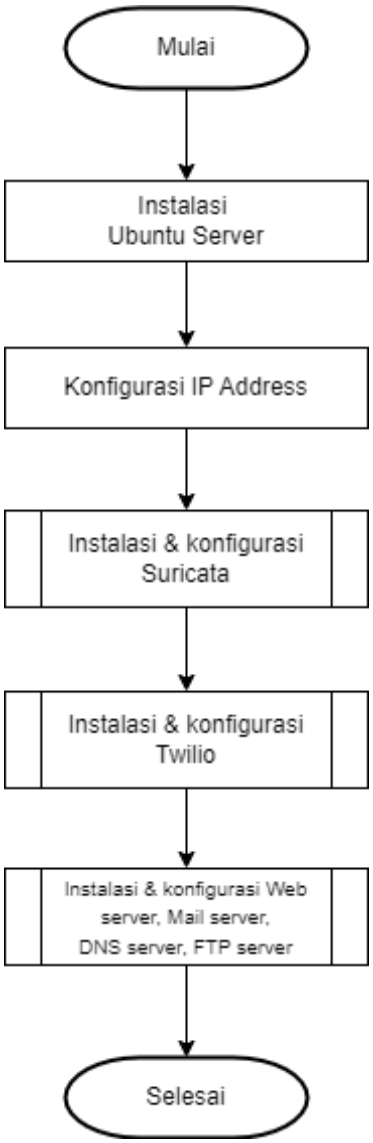
Gambar 3. 3 Flowchart Cara Kerja IPS Suricata

Gambar 3.3 di atas menjelaskan cara kerja IPS suricata di mana sistem akan melakukan pengecekan pada paket yang telah dikirim oleh penyerang dengan aturan yang telah dibuat pada masing-masing jenis serangan. Jika serangan tersebut

cocok (sesuai) dengan aturan, maka akan terdeteksi dan dilakukan tindakan dengan memblokir aktivitas yang mencurigakan tersebut. Tahap selanjutnya sistem akan memberikan notifikasi dalam bentuk pelaporan pada log yang sudah tersedia, yang di mana log tersebut dapat dipantau secara *real-time*. Jika lalu lintas jaringan yang terjadi dilakukan penyesuaian dengan *rules* dan hasilnya tidak sesuai maka tidak akan terdeteksi atau menandakan itu hanya lalu lintas jaringan biasa.

3.2.4 Implementasi

Gambar 3.4 menjelaskan bagaimana alur implementasi sistem pada penelitian ini, yaitu sebagai berikut:



Gambar 3. 4 Alur Implementasi Sistem

Gambar 3.4 merupakan alur implementasi sistem yang dilakukan tahap demi tahap dalam penelitian ini, yaitu sebagai berikut:

1. Langkah awal dari alur implementasi sistem adalah mempersiapkan *server* yang akan digunakan, dengan menginstal ubuntu *server* 22.04 yang digunakan sebagai *server* IPS suricata.
2. Peneliti akan mengatur konfigurasi IP address pada *server* tersebut agar dapat terhubung ke jaringan. IP address tersebut yang akan dijadikan sebagai IP target.
3. Peneliti selanjutnya akan menginstal dan mengkonfigurasi *tools* suricata yang berperan sebagai sistem keamanan IPS untuk mendeteksi dan memitigasi serangan siber yang nantinya akan diujikan pada penelitian ini. Untuk cara kerja dari *tools* ini sudah penulis jelaskan pada Gambar 3.4 diatas, serta dilakukan konfigurasi *rules* di dalamnya untuk setiap masing-masing serangan.
4. Pada penelitian ini menggunakan aplikasi whatsapp sebagai salah satu sistem notifikasinya, untuk dapat terhubung ke aplikasi whatsapp maka peneliti melakukan integrasi suricata dengan layanan yang tersedia pada *platform* twilio agar dapat mengirimkan notifikasi melalui aplikasi tersebut. Sedangkan untuk terhubung ke aplikasi telegram tidak harus menggunakan aplikasi atau layanan pihak ketiga.
5. Langkah terakhir peneliti akan menginstal dan melakukan konfigurasi berbagai layanan *server* seperti yang disebutkan di atas yaitu *Web server*, *Mail serv*er, DNS *server*, dan FTP *server* untuk sistem keamanan jaringan.

3.2.5 Monitoring dan Pengujian

3.2.5.1 Pengujian Validitas dan Reliabilitas

Pengujian validitas dan reliabilitas dalam penelitian ini dilakukan dengan teliti. Validitas diperoleh melalui pemilihan instrumen dan metode yang telah teruji, sedangkan reliabilitas dijaga melalui konsistensi hasil pengamatan, wawancara, dan analisis data log. Pengujian dilakukan untuk memastikan bahwa data yang diperoleh konsisten dan dapat dipercaya, sehingga kesimpulan yang dihasilkan dapat diandalkan sebagai dasar keputusan dalam mengimplementasikan sistem keamanan tersebut.

1. Pengujian Validitas

Pengujian validitas dalam penelitian ini dilakukan untuk memastikan bahwa instrumen yang digunakan, seperti IPS suricata serta notifikasi melalui telegram dan whatsapp, dapat mengukur variabel yang dimaksud dengan akurat. Validitas instrumen diuji dengan melakukan serangkaian uji fungsionalitas dan keandalan pada IPS suricata, termasuk mengonfirmasi bahwa sistem dapat mendeteksi dan mencegah berbagai jenis serangan siber yang relevan.

Selain itu, validitas notifikasi melalui telegram dan whatsapp diuji dengan memverifikasi bahwa notifikasi yang diterima oleh administrator secara akurat mencerminkan serangan yang terdeteksi oleh IPS suricata. Uji ini melibatkan simulasi serangan siber dan pengecekan respons notifikasi untuk memastikan bahwa informasi yang diberikan sesuai dengan jenis serangan yang terjadi.

Pentingnya validitas instrumen adalah untuk memastikan bahwa data yang dikumpulkan dapat diandalkan dan dapat dipercaya sebagai dasar untuk analisis dan kesimpulan penelitian. Oleh karena itu, pengujian validitas sangat diperlukan untuk memastikan bahwa metode yang digunakan dapat memberikan hasil yang sesuai dengan tujuan penelitian

2. Pengujian Reliabilitas

Dalam konteks penelitian ini, pengujian reliabilitas difokuskan pada keandalan dan konsistensi kinerja IPS suricata terhadap sistem notifikasi telegram dan whatsapp. Beberapa aspek penting yang diuji dalam pengujian reliabilitas melibatkan:

a. Konsistensi deteksi serangan yang dilakukan pada pengujian untuk memastikan bahwa IPS suricata memberikan hasil deteksi serangan yang konsisten pada situasi yang sama. Konsistensi ini menjadi indikator keandalan sistem dalam mendeteksi ancaman.
b. Stabilitas sistem notifikasi yaitu pengujian dilakukan untuk memeriksa stabilitas sistem notifikasi melalui telegram dan whatsapp. Keandalan notifikasi dievaluasi dengan memastikan bahwa pemberitahuan yang dikirimkan secara konsisten dan tepat waktu setiap kali terjadi serangan.
c. Reprodusibilitas hasil pengujian di mana penting untuk menjalankan pengujian secara berulang dan membandingkan hasilnya untuk memastikan

bahwa hasil yang diperoleh dapat direproduksi. Hal ini menunjukkan bahwa kinerja IPS suricata dan notifikasi telegram dan whatsapp bersifat konsisten.

d. Kemampuan respons sistem yaitu pengujian dilakukan untuk mengukur sejauh mana sistem dapat merespons secara konsisten terhadap serangan siber. Waktu respons dan efisiensi dalam mengatasi serangan menjadi fokus utama dalam mengukur reliabilitas

Pengujian reliabilitas ini diperlukan agar hasil yang diperoleh dari penelitian dapat diandalkan dan dapat digunakan sebagai dasar untuk mengambil keputusan terkait implementasi IPS suricata serta notifikasi telegram dan whatsapp dalam konteks keamanan siber. Dengan memastikan keandalan dan konsistensi, dapat dipastikan bahwa sistem yang diusulkan dapat berfungsi efektif dalam mendeteksi dan mengatasi serangan siber.

3.2.5.2 Rancangan Pengujian Hipotesis

Rancangan ini bertujuan untuk menguji hipotesis yang diajukan dalam penelitian. Sebagai contoh, salah satu hipotesis yang dapat diuji adalah "Implementasi *Intrusion Prevention System* Suricata meningkatkan efektivitas deteksi serangan siber." Metode pengujian statistik, seperti uji t atau uji *chi-kuadrat*, akan digunakan untuk mengevaluasi signifikansi hasil dan menyimpulkan apakah hipotesis dapat diterima atau ditolak. Ini memberikan dasar ilmiah untuk menyatakan sejauh mana implementasi IPS suricata dan notifikasi telegram dan whatsapp efektif dalam mengamankan sistem dari serangan siber.

Dengan demikian, rancangan analisis data ini akan memberikan pemahaman yang lebih mendalam tentang hasil pengujian dan sejauh mana temuan penelitian mendukung hipotesis yang diajukan.

3.2.5.3 Skema Pengujian

Berikut merupakan skema pengujian serangan dalam penelitian, setiap langkah dirancang untuk mensimulasikan serangan siber yang berbeda untuk mengevaluasi seberapa efektif suricata sebagai IPS atau sistem deteksi dan mitigasi intrusi. Pengujian mencakup serangan yang biasa digunakan untuk mengganggu keamanan jaringan dan sistem. Berikut penjelasan secara detail untuk setiap jenis serangan, disajikan dalam poin-poin:

1. Pengujian pada serangan ICMP *Flood* yaitu dengan membuat paket ICMP dalam jumlah besar untuk membanjiri *server* target, mensimulasikan serangan DoS untuk menilai kemampuan suricata dalam mendeteksi dan mitigasi serangan tersebut.
2. Pengujian pada serangan DDoS *Attack* dilakukan dengan beberapa sistem yang digunakan untuk membanjiri *server* target dengan trafik, serangan akan menghabiskan sumber daya dan mengganggu layanan. Efektivitas suricata dalam mendeteksi dan mencegah serangan DoS terdistribusi akan dievaluasi.
3. Pengujian pada serangan *Port Scanning attack* yaitu dengan menyelidiki *server* target untuk mengetahui *port* dan layanan yang terbuka, menggunakan teknik pemindaian pada setiap *port*. Hal tersebut menguji kemampuan suricata dalam mengidentifikasi dan memperingati aktivitas pengintaian.
4. Pengujian pada serangan IP *Spoofing Attack* yaitu dimana paket-paket berbahaya menggunakan Alamat IP sumber palsu dikirimkan ke *server* target untuk menguji kemampuan suricata dalam mendeteksi dan memblokir paket-paket yang berusaha menyamarkan asal usulnya.
5. Pengujian pada serangan XSS *Attack* yaitu dilakukan dengan menyuntikkan *script* berbahaya ke dalam halaman web yang dilayani oleh *server* target. Bertujuan untuk menilai efektivitas suricata dalam mendeteksi dan mitigasi serangan injeksi kode dari sisi klien.
6. Pengujian pada serangan SQLi yaitu dilakukan dengan menyuntikkan perintah SQL melalui *input* aplikasi *web* untuk dapat manipulasi pada *database*.
7. Pengujian pada serangan *Slow* HTTP *attack* dilakukan dengan mengirimkan permintaan HTTP yang sangat lambat ke *server* target, bertujuan untuk menghabiskan sumber daya *server* dengan koneksi yang tidak lengkap.
8. Pengujian pada serangan SYN *Flood attack* dilakukan dengan mengirimkan banyak paket SYN palsu ke *server* target, bertujuan untuk menghabiskan sumber daya *server* dengan koneksi TCP yang tidak lengkap.

Pada setiap tahapan dalam skema pengujian akan melibatkan pemantauan dan pencatatan secara rinci terhadap kemampuan deteksi suricata, serta respon sistem terhadap setiap jenis serangan. Dimana hasil akan dianalisis untuk menentukan kekuatan dan kelemahan suricata dalam melindungi dari berbagai ancaman siber.

3.3 Alat dan Bahan Penelitian

3.3.1 Alat Penelitian

Untuk mempermudah proses eksperimental dan analitik, serangkaian instrumen dan perangkat lunak khusus digunakan dalam penelitian. Serangkaian alat diperlukan untuk membangun pengaturan eksperimental, melaksanakan eksperimen, mengawasi aktivitas jaringan, mengidentifikasi gangguan, dan mengevaluasi data yang dikumpulkan. Setiap alat yang digunakan sangat penting untuk dapat mencapai tujuan penelitian yang tepat dan dapat diandalkan. Tabel 3.1 memberikan informasi yang tepat tentang alat yang digunakan dalam bentuk perangkat keras.

Tabel 3. 1
Informasi Perangkat Keras

No	Perangkat Keras	Spesifikasi	Deskripsi
1.	PC #1 (*server*)	AMD Ryzen 5 5600H Radeon Graphics 3.30 GHz, 3301 MHz, 6 Core (s), 16 GB RAM	Perangkat digunakan sebagai *server* yang sudah terinstall IPS suricata di dalamnya.
2.	PC#2 (penyerang)	-	Perangkat digunakan sebagai penyerang untuk melakukan penyerangan.

Pada penelitian ini juga dilakukan dengan bantuan menggunakan perangkat lunak yang dapat dilihat pada Tabel 3.2, sebagai berikut:

Tabel 3. 2
Informasi Perangkat Keras

No	Perangkat Lunak	Spesifikasi	Deskripsi
1.	*Operating System* PC *1	Ubuntu *server* LTS 22.04.4 (64-bit)	Sistem operasi ini digunakan dalam penelitian sebagai *server* IPS.
2.	*Operating System* PC *2	Kali Linux 2023.4 (64-bit)	Sistem operasi ini digunakan dalam penelitian sebagai penyerang.
3.	Suricata	*Version 7.0.5*	Perangkat lunak ini digunakan dalam penelitian untuk mendeteksi dan mitigasi serangan.
4.	Wireshark	*Version 4.2.2*	Perangkat lunak ini digunakan dalam penelitian untuk melakukan monitoring lalu lintas jaringan.
5.	*hping3*	*Version 3.0.0-alpha-2*	Perangkat lunak ini digunakan dalam penelitian untuk mengirim paket jaringan.
6.	*Python Script*	*Version 3.10.12*	Perangkat lunak atau Bahasa pemrograman yang digunakan untuk melakukan pengolahan dan analisis log.
7.	*LOIC*	-	Perangkat lunak ini digunakan dalam penelitian untuk melakukan serangan

			DDoS *(Distributed Denial of Service).*
8.	*Web Server*	*Version 2.4.52 (ubuntu)*	Perangkat lunak ini dalam penelitian melibatkan pengujian dan mitigasi serangan.
9.	*FTP Server*	*Version 3.0.5*	Perangkat lunak ini dalam penelitian melibatkan pendeteksian dan mitigasi serangan.
10.	*Database Server*	*Version 8.0.36*	Perangkat lunak ini dalam penelitian melibatkan pengujian dan mitigasi serangan.
11.	*Mail Server*	*Version 3.6.4*	Perangkat lunak ini dalam penelitian melibatkan pengujian dan mitigasi serangan.

3.3.2 Bahan Penelitian

Bahan penelitian yang digunakan dalam penelitian ini adalah buku elektronik, publikasi ilmiah, jurnal akademis, dokumentasi resmi, dan situs internet. Dengan tujuan untuk mengidentifikasi dan mengurangi serangan siber sumber-sumber tersebut memberikan wawasan tentang pembuatan dan penerapan IPS suricata. Untuk membantu analisis dan penilaian lebih lanjut, digunakan data eksperimental dari simulasi serangan dan penangkapan lalu lintas jaringan.